(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11527 A2

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/21615

(22) International Filing Date: 8 August 2000 (08.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/148,183 10 August 1999 (10.08.1999) US

(71) Applicant *(for AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IL, IT, JP, LU, MC, NL, PT, SE only)*: **YEDA RESEARCH AND DEVELOPMENT CO. LTD.** [IL/IL]; P.O. Box 95, 76100 Rehovot (IL).

(71) Applicant *(for CA only)*: **FLEIT, Lois** [US/US]; 520 Brickell Key Drive #A201, Miami, FL 33131 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PINKAS, Binyamin** [IL/IL]; Eibeshitz Street 6, 62741 Tel-Aviv (IL). **NAOR, Simeon** [IL/IL]; Beit Street 5, 69122 Tel-Aviv (IL).

(74) Agents: **FLEIT, Martin** et al.; Fleit Kain Gibbons Gutman & Bongini, 520 Brickell Key Drive #A201, Miami, FL 33131 (US).

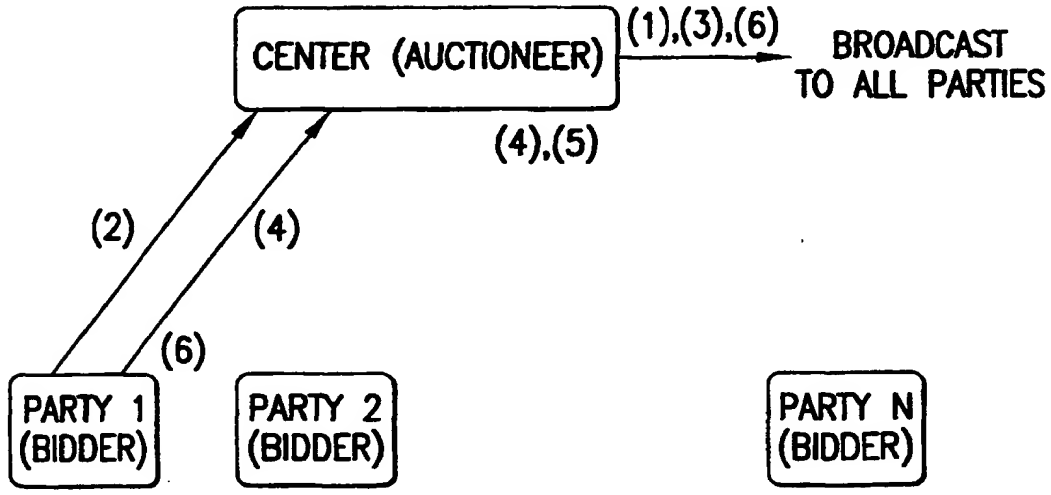
(81) Designated States *(national)*: CA, IL, JP, US.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: HONESTY PRESERVING NEGOTIATION AND COMPUTATION



(57) Abstract: A method and system for preserving the integrity of a negotiation that includes providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n. Each user B.sub.i generates an input X.sub.i, which is input to the center A. The center A computes and publishes a function F(X.sub.1,X.sub.2,...,X.sub.n) based on the input messages it receives. Each user B.sub.i (1<=i<=n) communicates with the center A, exclusively. Center A publishes additional information which lets each of the users verify that F was computed correctly, and prevents a coalition of any one subset of the users from learning anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, or information about the inputs of other users.

WO 01/11527 A2

HONESTY PRESERVING NEGOTIATION AND COMPUTATION

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates generally to cryptography and to secure distributed computation, and more particularly it relates to computerized auctions conducted using PCs and/or servers over a network, such as, the Internet.

Description Of The Prior Art

An exciting topic of cryptographic research is secure function evaluation [see e.g. REFERENCES 3, 7, the citations for which are given in detail at the end of the specification]. For any function F(x.sub.1, x.sub.2,...,x.sub.n), it is possible, in principle, to construct a protocol that allows a group of n parties, where party i has as its private input x.sub.i, to jointly evaluate F(x.sub.1, x.sub.2,...,x.sub.n). Following the protocol the parties learn F(x.sub.1, x.sub.2,...,x.sub.n) but no party i can learn about the inputs other than x.sub.i more than can be computed from x.sub.i and F(x.sub.1, x.sub.2, ..., x.sub.n). The drawback of these protocols is that they are rather complex and require a lot of interaction between each of the parties. In the case of auctions this would require high interaction between the bidders, who have no motivation to interact with each other. The present invention, as will be described in greater detail in the following, provides a much simpler method in which all the parties communicate with just a single center. In the inventive method described hereinafter, the input of each of the parties becomes known to this center but otherwise, it is not known to any other party. The inventive method enables the center to prove that it preformed the computation correctly.

In the case of auctions, it is normally the case that the auctioneer is trusted by all parties to compute the result of the auction correctly. This might not be justified, since the auctioneer might benefit from an illegal modification of the result of the

auction. (This is even true if the auctioneer is just a mediator that is selling items which are offered by third parties, since such auctioneers usually charge a commission which depends on the price with which the items are sold). It is sometimes the case that a trusted party (say an accountant) observes the operation of the auctioneer and testifies that it is trustworthy. However this party might be corrupted and cooperate with a corrupted auctioneer, it might also be the case that the trusted party cannot watch the auctioneer closely enough and the auctioneer can cheat without being detected. These problems are amplified in a computerized Internet setting.

The center that computes F can of course prove that it computed it correctly by publishing all the inputs. However this solution affects the privacy of the other parties, since their inputs become public. The inventive method overcomes this problem since it enables the center to prove that it computed F correctly without leaking any information about the inputs.

There are suggestions in the art for distributing the operation of an auctioneer between many servers in a way which is secure as long as not too many of these servers operate maliciously. Franklin and Reiter [see REFERENCE 2] developed a distributed system for sealed-bid auctions with many auctioneer servers, which ensures the privacy of the bids until the time they are opened. This system further enables the bids to be backed by escrowing financial commitments of the bidders. Harakavy, Tygar, and Kikuchi [see REFERENCE 4] present systems for secure first price and second price sealed bid auctions, which preserve the privacy of the bids even after the winning bid is chosen (this variant was also briefly mentioned in REFERENCE 2). Both systems distribute the operation of the auctioneer between several servers and privacy is guaranteed as long as not too many of the servers collude (most of the protocols require that less than a third of the servers collude, and therefore, need a minimum of four servers). However, if enough auctioneer servers collude they are able to maliciously change the outcome of the auction and would not be detected. The requirement that auctioneer servers would not collude seems very hard to enforce since all these servers operate for the auctioneer which might have a motivation to cheat and increase its profits. Compared to these prior art solutions, the inventive method does not require to distributing the operation of

the auctioneer among several non-colluding servers, and provides security even if the auctioneer is attempting to cheat.

Naor and Pinkas [see REFERENCE 6] present a different method that prevents even the center from learning information about the parties' inputs. That method requires the operation of an additional party - the Issuer. The Issuer generates a program that computes the function (or the auction) and sends it to the center. The center receives messages from the parties, which contain some information that is intended for the Issuer. After the center receives messages from all the parties it sends a message to the Issuer and receives a response which enables it to use the program to compute the output of F for the parties' inputs. The method ensures that neither the center nor the Issuer learn information about the inputs of the parties. In this sense it provides better privacy than the inventive method described herein. However, the inventive method presented here does not require the cooperation of any additional party (like the Issuer) for the computation of F. It enables the center to compute the function by itself and prove that it computed it correctly, and in this respect is an advantage.

SUMMARY OF THE INVENTION

Consider a scenario with N parties, each having a private input, and a single center. There is a function F with N inputs whose output should be computed. Each party sends its input to the center. The present invention is a method, system and apparatus that enables the center to compute and publish the output of F and to prove to all parties that it computed F correctly. This is done without revealing the value of the input of a party to any other party.

More specifically, the parties can be bidders in an auction, their inputs are their bids, the center is the auctioneer, and the program F expresses the rule by which the outcome of the auction is decided. The invention requires the auctioneer to prove that it computed the result of the auction correctly.

The invention provides the same security as in the following scenario: Assume that there is a reliable party (say an accountant or a lawyer) which is trusted

by all other parties. This party observes the operation of the center, i.e. it examines the inputs that the center receives, verifies that the center computes the correct output, and testifies that this is the case. The invention provides the same security as is provided with this trusted party, but without using any such party. This ensures better security (since trusted parties might breach the trust they are given), and is more efficient (since it does not require an additional party).

Other and further advantages and objects of the present invention will become readily apparent when considering the following detailed description of the present invention when taken together with the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the different entities engaged in a computerized auction.

Figure 2 is a schematic diagram illustrating the steps of the method of the present invention where the steps are indicated by numerals in parentheses.

Figure 3 is a high level descriptive flow chart of the present invention as generally depicted in the diagrams of Figures 1 and 2.

Figures 4A and 4B are a flow chart showing the steps of the implementation of the preferred embodiment of the present invention.

Figure 5 is a flow chart of a secure two-party function evaluation protocol as implemented by the present invention.

Figure 6 is a schematic diagram of a gate used in the protocol depicted in Figure 5, and also shows the pseudo-random function used to prepare Table T_g used in the protocol of depicted in Figure 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

As initially noted, the apparatus and method of the present invention comprises an auction service that is used in a network, such as, the Internet, and uses clients and/or servers. The invention utilizes cryptography and secure distributed computation via computers to effect a computerized auction. However, the invention is not limited to computerized auctions, but has broader application.

Many such applications involve a group of participants, denoted herein as "Parties", each of whom has an input to the group as a whole, where the group as a whole is required to compute and output a certain function of these inputs. The term "function" herein denotes, in the usual sense, any mathematical or logical mapping from one set of input entities to an output entity or set of entities. In certain cases, the inputs may involve sensitive information, such that it would also be required that this computation does not reveal any information about the inputs, except for whatever might be computed from the final output. Such inputs are herein denoted as "private inputs". If, in addition to the parties, there were furthermore a trustworthy participant, denoted herein as a "center" and which is trusted by all the parties, then each party could simply send the respective private input to this center, which would then compute the function and publish, or output, the value of the computed function. (The center is a participant in the protocol and is involved in the computation of the function. It may or may not have a private input, and may or may not be within the group of parties.) The parties, however, might not trust each other, and might not trust any single center.

Although a particular case of interest is that of auctions, for example, sealed-bid second-price auctions, commonly known in the art as "Vickrey auctions", other applicable activities include mechanism design, which deals with the design of protocols for selfish parties. The goal of a protocol is to aggregate the preferences of the parties in order to decide on some social choice (for example, to decide whether a community should build a bridge, or how to route packets in a network, or to decide who wins an auction). Each party has a utility function which expresses how much that party values each possible outcome of the protocol (the bid in an auction, for example, is such a utility function). Each party sends information about its utility function to a center, which decides on the outcome of the protocol based on the reports from the parties, according to a specified function of the utility functions (for example, in a sealed-bid auction, the specified function that determines the winner is the maximum of the bids). The creation of algorithms by mechanism design is known in the art, to solve a global problem among a number of selfish agents (e.g. routing, or some cooperation between the agents). The present invention can be used to compute these algorithms without requiring trust in the center. The plausibility of using the present invention for such a task depends on the

complexity of expressing the utility functions and decision procedure in terms of circuits.

A particular case of interest is the Groves-Clarke mechanism, where the public good is served if the sum of reported values is higher than some threshold. The circuit which computes this function is very simple, as is the circuit which computes the sum of the reported values for several options, and decides on the option with the highest sum. It is therefore very easy to use the present invention to provide a private protocol which computes a Groves-Clarke mechanism.

Opinion polling is another relevant application. The design of mechanisms to elicit opinions of a group of independent experts. The application enables parties to contribute their opinion to a decision making without being worried that their opinion would be revealed. It is known in the art that where experts want their recommendation to be accepted, that there exists a mechanism with a single equilibrium which achieves the public target (but such a mechanism does not exist if experts care only about the public good). Such a mechanism can be implemented very efficiently by the present invention. This essentially requires that one expert chooses a subset of the experts whose opinions are considered, learns their opinions, and then adds his opinion. The group decision is the majority opinion.

Another application is for polling the opinions of a group of people, while hiding the individual opinions of the participants. Consider for example an opinion poll (such as the Gallup Poll) which contains many questions. Suppose that the poll is anonymous, and the organizer obtains lists of answers, one list for each participant. In order to prove that it computed the result correctly, the organizer must publish the lists of answers. Suppose also that only a single participant answered affirmatively to a certain question, and that it is possible to guess with very high probability who this participant is. Then, although the answers are anonymous, it is possible to learn the answers of this participant to all the questions. The present invention enables the sending of questions to the group members, and the processing of their answers to obtain commutative outputs without revealing any information about individual answers. Additional applications of the present

invention include multiple-question opinion polls, sociometric research, and voting and elections.

Stable matching is yet another example of a global decision which depends on the private preferences of many parties. In many scenarios it is plausible that parties would be hesitant to reveal their matching preferences, even to the center that computes the matching (consider, for example, matching couples for a prom). The present invention enables the parties to reveal their true preferences without being afraid that the center can learn them. As with other applications, the overhead of implementing the present invention for this application depends on the complexity of expressing the matching algorithm as a combinatorial circuit.

Referring now to the drawing, the different entities are depicted in Figure 1. As shown, the entities include **The parties 320** and the **Center 321**. Each of the parties **320** has an input to the function F. In the case of auctions some of the parties might wish to sell items, and the rest of the parties are interested in buying these items. In addition to the parties 320, there is a **center 321.** The center **321** runs the show: it advertises the fact that F is computed, receives the inputs, and performs the computation. In the case of auctions, the center is the auctioneer. It publishes the auction, receives the bids from the bidders, and computes the outcome of the auction. The auctioneer might be a party which merely organizes the auction. It is also possible that it is one of the bidders or one of the sellers (for example he is selling an item which all other bidders are interested in buying).

The Steps in a high level description of a preferred embodiment are illustrated in Figure 2. The high level description of the illustrated preferred embodiment of the method involves the following sequence of steps of the protocol. The Steps include the following sequence. (1) The center announces the computation and commits to the circuits. (2) Party 1 sends a commitment to its input (Party 1 represents a generic party, and this operation is performed by each of the participating parties). (3) The center publishes the commitments. (4) Party 1 opens its commitment, and the center

verifies it. (5) The center computes the function. (6) The center publishes a proof that the computation was correct, and Party 1 verifies it.

The Steps of the method of the present invention are elaborated in more detail in the following, with reference to Figure 3. As shown, there are a number of bidders 320 and a single center 321. The center announces Step **301** that it will compute the function F. (In the case of an auction the auctioneer announces the existence of the auction and publishes its rules). The center publishes in Step **302** commitments to K combinatorial circuits **322** that compute F (where K is a security parameter).

Party B.sub.i, which wishes to participate in computing the function F, sends a message to the center. They might exchange several rounds of communication, Step **303,** at the end of which the center has a commitment c.sub.i to the value of B.sub.i's input x.sub.i.

The center publishes in Step **304** the commitments it received from the parties. (In the case of auctions this can be done at the end of the bidding period).

In Step **305** the bidders choose part of the K circuits that the center committed to, from block **323,** and ask the center to open them. They verify in Step **306** that the circuits compute the function F. In Step **307** each party B.sub.i sends to the center the value x.sub.i to which it committed with c.sub.i. The center verifies that x.sub.i corresponds to c.sub.i, that is it verifies that A(x.sub.i,c.sub.i)=1.

The center now computes in Step **308** the value of the circuit that computes F for the inputs x.sub.i it received. Next, the procedure for verifying the computation takes place. The center computes and publishes a proof in Step **309** that it computed the value of F correctly. Each party can use the published commitments to verify in Step **310** that the proof is correct.

A considerable improvement to the protocol can be achieved by noting that the function that is computed by the circuit need not be the function F that the center

computes, and whose computation should be verified. The circuit can compute a function F' that **verifies** that F was computed correctly. For example, if F is a function that computes the value and the index of the maximum of N inputs, X(1),...,X(N), F' is the following function: It has N+2 inputs comprised of the N inputs to F and the outputs (j,Y) of F. F' outputs 1 if and only if X(j)=Y, and X(j)>=X(i) for every i different from j. The circuit that computes this function is substantially more efficient that the circuit computing F.

There now is elaborated a detailed description of the preferred embodiment . The inventive method employs cryptographic tools that enable a secure two-party function evaluation. The particular secure two-party function evaluation protocol used in the present invention is based on the method disclosed in REFERENCE 7. In the invention, the protocol is run between two participants, ***A*** and ***B***. The input of ***A*** is a value *x* and the input of ***B*** is a description of a function ***f***. At the end of the protocol, ***A*** learns ***f***(*x*) (but no other information about ***f***), and ***B*** learns nothing about *x*. Thus, the input *x* is a private input of ***A***, and the function ***f*** is a private input of ***B***.

The protocol is based on expressing ***f*** as a combinatorial circuit of gates which are over some fixed base (e.g. all the functions **g**: 0,1 times 0,1 to 0,1). The bits of the input are entered into input wires and are propagated through the gates.

This procedure encrypts a circuit by generating a pseudo-random isomorphic transformation of the circuit. This encryption is herein referred to as a "garbling" of the circuit. The cyphertext of a circuit so encrypted by this procedure is herein denoted as a "garbled" circuit. This process is detailed below, with reference to Figure 5.

As shown in Figure 5, Inputs **502** include: ***A:*** a value *x*, in an input **502-A**, and ***B:*** a description of a combinatorial circuit which computes ***f***, in an input **502-B**. The outputs of the flowchart shown in Figure 5 are Outputs **536** that include: ***A:*** ***f***(*x*), in an output **536-A**, and ***B:*** nothing, in an output **536-B**.

The protocol starts with Initialization. In step **504, *B*** devises a circuit **506** made of logic gates, such that circuit **506** computes ***f***. The design of logic circuits made of gates that compute functions is well-known in the art.

Next, the circuit is encrypted. In step **508, *B*** assigns to each wire i of circuit **506** two random values (W_i^0, W_i^1) **510** corresponding to 0 and 1 values of wire i. The random values should be long enough to be used as keys (for example, 80 bits long). The value of wire i is denoted by b_i. In step **512, *B*** also assigns to wire i a random permutation π **514** over 0,1, π_k: $b_i \rightarrow c_i$.

In step **516, *B*** uses a pseudo-random function R **518** to prepare a table T_g **522** (or a set of tables, also denoted herein by T_g) which enables computation of the garbled output of each gate **g 520**, $(W_k^{b_k}, c_k)$, from the values $(W_i^{b_i}, c_i)$, $(W_j^{b_j}, c_j)$, the garbled inputs to gate **g**. Table T_g does not disclose any information about the output of gate **g** for inputs other than the pair (b_i, b_j), nor discloses the values of the bits b_i, b_j, or b_k.

In step **524, *B*** prepares an output translation table T_O **526** which decrypts the garbled output bits of the circuit (the cyphertext output) to the actual bits of the output of the circuit (the cleartext output).

Figure 6 illustrates gate **g 520**, which is a generic gate that computes the value b_k of an output wire k **604** as a function of the values b_i, and b_j of input wires i **606** and j **608**, respectively. Such a computation is denoted as $b_k = \mathbf{g}(b_i, b_j)$. Figure 6 also illustrates pseudo-random function R **518**, which is used to prepare table T_g **522**.

If one assumes initially that the fan-out of every gate is 1, table T_g contains four entries of the form:

$$c_i, c_j: (W_k^{g(b_i, b_j)}, c_k) \text{ XOR } R_{W_i^{b_i}}(c_j) \text{ XOR } R_{W_j^{b_j}}(c_i),$$

where $0 \le i \le j \le 1$.

The value c_k is given by $c_k = \pi_k(b_k) = \pi_k(g(b_i, b_j))$. The entry does not have to include the index c_i, c_j since this is implicit in the entry's location.

Assume that ***A*** knows c_i, c_j and the values $W_i^{b_i}$, $W_j^{b_j}$. In order to compute a gate, ***A*** finds the entry c_i, c_j in the table T_g for that gate, and performs an XOR (exclusive-OR) operation with the value $R_{W_i^{b_i}}(c_j)$ XOR $R_{W_j^{b_j}}(c_i)$ to get the value $W_k^{b_k} = W_k^{g(b_i, b_j)}$, and of c_k.

To code the Input the following is undertaken. Given the table T_g of the gates, and the garbled values $W_i^{b_i}$ and c_i which correspond to the input wires, it is easy to compute the garbled values of the output wires of the circuit. ***A*** knows the values of the input bits and should obtain the values of the corresponding wires. In step **528**, for each gate in circuit **506**, ***B*** sends to ***A*** the table T_g **522** that codes the gate. In step **530**, ***B*** sends to ***A*** the table T_O **526** that decrypts the garbled values of the output of the circuit the output bits of the circuit. In step **532**, for each gate input wire in the circuit, ***A*** and ***B*** engage in an Oblivious Transfer, at the end of which ***A*** learns the garbled value of the wire's input bit (but nothing about the garbled value of the input bit of the other wire into the gate), and ***B*** learns nothing.

A now has enough information to compute the circuit. In step **534**, ***A*** computes the output of the circuit for the input x. However, since ***A*** does not know the garbled values for any other input bits, ***A*** cannot compute information about $f(x_0)$ for any $x_0 \neq x$ (except, of course, information that can be deduced from $f(x)$ alone). Note that the communication between the two participants ***A*** and ***B*** can be done in a single back-and-forth round, and ***B*** can prepare the circuit in advance, before the input is known to ***A***.

To handle a gate fan-out greater than 1, it is simply required to use a different input to the pseudo-random function R at each gate in which the wire is used. (If the same value be used in different gates, then it will be possible to cancel the application of the pseudo-random function R by an XOR operation, and ***A*** could thereby learn relationships between garbled values.) Suppose that the fan-out of wire i is M, then in a gate m ($1 \leq m \leq M$) which uses wire i as input, the masking value that is used should be $R_{W_i^{b_i}}(c_i, m)$. That is, the pseudo-random function R

should be applied to the concatenation of c_j and m. Alternatively, it is possible to assign each gate a unique identifier I_g, and use $RW_i^{bi}(c_j, I_g)$.

It is also possible to adapt this protocol to circuits in which gates have more than two inputs, as well as, for wires having more than two possible values. The size of the table for a gate with n inputs which each can have d values is d^n.

The prior art of REFERENCE 7 (Yao's protocol) is limited to two participants, but has been extended has been extended in the prior art to handle multi-party inputs, see REFERENCE 3.. These extended protocols, however, require a round of communication for each gate in the circuit, which is impractical in many applications, such as in auctions. The method of REFERENCE 3 would require extensive interactive communication among the bidders in an auction, and is therefore not suitable. In contrast, the present invention does not impose the burden of extensive interactive communication and does not require the bidders to communicate among themselves, and therefore represents an improvement not only over the prior art of REFERENCE 7 and 3. Furthermore, the prior art of REFERENCE 3 is secure only for limited coalitions of less than one-third of the parties.

A commitment to a value X is similar to the following process: party B which knows the value of X writes it on a piece of paper which is put in a sealed envelope. At this stage no one can learn anything about X, but B is committed to X and cannot change the value in the envelope. At a later stage B can "open the commitment" by opening the envelope and revealing X.

More formally, a commitment to a value X is computed by a function C=C(X,R), where R is a random string. It has the following properties: (1) C is easy to compute. (2) Given C(X,R), it is infeasible to compute any information about X. (3) There is an algorithm A such that A(C(X,R),X,R)=1, and for any other X' (different than X) and R' it holds with high probability that A(C(X,R),X',R')=0. Such commitments schemes can be implemented efficiently, see for example REFERENCE 5.

Now the details of the implementation of the preferred embodiment will be described in conjunction with the flow chart of Figures 4A and 4B. The first stage is the announcement. This stage is carried out by the center **421** announcing in step **401** that it will compute F. Let K be a security parameter. The center constructs in step **402** K garbled circuits that compute F. For each input wire j of each of the circuits the center chooses in step **403** a random permutation P.sub.j over the two values 0 and 1. The center publishes in step **404** the tables of the gates of the K circuits **422**. For each input wire j (in each of the circuits) it publishes in step **404** a commitment to W.sub.j.sup.0 and a commitment to W.sub.j.sup.1, ordered by the permutation P.sub.j, and a commitment to P.sub.j.

The next stage is for the parties 420 to commit to their inputs. Each party B.sub.i has an input x.sub.i of l bits. The bits of this input are denoted as x.sub.(i,l). Each input bit should be input to an input wire in each of the K circuits. For each wire j of these wires, the center sends in step **405** to B.sub.i, the permutation P.sub.j. B.sub.i sends in response in step **406** a commitment **424** to P.sub.j(x.sub.(i,l)), i.e. to the permuted value of its input.

The next stage is to publish the commitments. The center **421** publishes in step **407** the commitments **424** it received from the parties.

The next stage is to open the commitments. The parties **420** choose K/2 of the K circuits that the center has created and ask the center to open in step **408** all the commitments to the permutations and garbled inputs of these K/2 circuits **423**. They verify in step **409** that these circuits indeed compute F. Each of the parties B.sub.i sends in step **410** its input x.sub.i to the center. B.sub.i also opens to the center the commitments that it made to each of its assigned input wires. These were for values 0 or 1 which are the permuted values of B.sub.i's inputs. The center verifies in step **411** that these commitments are consistent. The center publishes in step **412** the opened commitments **425** of each of the parties, and opens the garbled values W.sub.j.sup.0 or W.sub.j.sup.1 that correspond to them.

In the next stage, the center computes the function in step **413** and publishes the output of each of the K/2 circuits which were not chosen by the

parties.

In the final stage, each party **420** can verify the computations of the center **421.** Each B.sub.i can use the opened garbled values **425** and the tables of the gates **422** to compute the output of each of the K/2 circuits, and verify in step **414** that they all have the same output.

One problem that may be encountered in an auction is that a party does not open its commitment. For example, a party might refuse to communicate with the sender at the step at which the commitments should be open. This type of behavior enables cheating, for example, in the case of second price auctions the center itself might use fake identities of bidders in order to commit to bids in different values, and open only the bids which are smaller than the highest value among all other bids. This behavior might increase the amount that the winner would be required to pay.

One approach for dealing with parties that do not open their commitments appropriately would be to require parties to also submit their bids to a trusted third party T. The help of the trusted party T is not required, if all parties open their commitments. However, when a party refuses to open its commitment, the trusted party T can be called upon to open it. Such a scheme can be realized, for example, by using commitments of the following form: the public key of trusted partyT would be known to everyone. A commitment to a value v would be an encryption of this value with T's public key (say with a probabilistic encryption scheme which ensures indistinguishability). The party who created this commitment can open it by revealing v and showing how it encrypted it. If this party refuses to open the commitment then trusted party T can open it using its private key.

A more promising approach is to use "Timed commitments" [see REFERENCE 8]. These are commitment schemes with an optional forced opening phase enabling the receiver of the commitment to recover (with effort) the committed value without the help of the bidder making the commitment (committor). It is possible to require the bidders to use timed commitment schemes to commit to their bids, enabling the auctioneer to open these commitments, to their original value, if a bidder is not willing to open his or her bid.

A different approach for ensuring that each party opens its commitments is to require parties to back their commitments financially. A party who refuses to open its commitment would be required to pay a fine.

References

[1] M. Bellare and S. Micali, Non-interactive oblivious transfer and applications, Proc. Advances in Cryptology - Crypto '89, Springer-Verlag LNCS 435 (1990), 547-557.

[2] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction server", IEEE Tran. on Software Engineering, 22(5), pp. 302-312, 1996.

[3] O. Goldreich, M. Micali, A. Wigderson, How to play any mental game, Proc. 19th ACM Symp. on Theory of Computing, 1987, pp. 218-229.

[4] M. Harakavy, J. D. Tygar and H. Kikuchi, "Electronic auctions with private bids", 3rd USENIX Workshop on Electronic Commerce, pp. 61-73, 1999.

[5] M. Naor, "Bit Commitment using Pseudo-randomness", J. of Cryptology, 4, 1991.

[6] M. Naor and B. Pinkas, "Privacy preserving negotiation and computation", patent application, 1999.

[7] A.C. Yao, How to Generate and Exchange Secrets, Proc. of the 27th IEEE Symp. on Foundations of Computer Science, 1986, pp. 162-167.

[8] D. Boneh and M. Naor, "Timed commitments and timed signatures", Proc. Advances in Cryptology - Crypto '00, Springer-Verlag LNCS, 2000.

Although the invention has been shown and described in terms of specific embodiments, nevertheless various changes and modifications will be evident to those skilled in the art from the teachings of the invention. Such changes and modifications which do not depart from the spirit, scope and contemplation of the invention are deemed to fall within the purview of the claims.

WHAT IS CLAIMED IS:

1. A method for preserving the integrity of a negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n,

b) generating for each user B.sub.i an input X.sub.i,

c) inputting each user's input X.sub.i to the center A,

d) computing and publishing a function F(X.sub.1,X.sub.2,...,X.sub.n) by the center A based on the input messages it receives,

e) each user B.sub.i (1<= i<= n) communicating with the center A exclusively, and

f) publishing by center A additional information which lets each of the users verify that F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, and (ii) information about the inputs of other users.

2. The method of Claim 1 for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount he has to pay.

3. The method according to any one of claims 1 or 2, for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount to be paid, and wherein the center only makes disclosure to the winning bidder, while all other bidders being able to verify that the auction was computed correctly, but do not learn any other information.

4. The method according to any one of claims 1, 2 or 3, for first price auctions, where the output of F is (B.sub.j, X.sub.j), where X.sub.j is greater or equal to any one X.sub.i for 1 <=i <=n.

5. The method according to any one of claims 1, 2 or 3, for second price auctions (Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1.

6. The method according to any one of claims 1, 2 or 3, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1 <=i <=n.

7. The method according to any one of the preceding claims wherein the auction is a plural auction where there are a plurality of sellers.

8. The method according to any one of the preceding claims wherein the auction is a generalized Vickrey auction.

9. The method according to any one of the preceding claims, comprising the step of, computing the auction such that the auctioneer wants to buy an item and each of the bidders wants to sell this item, and wherein negative values of the inputs X.sub.i are possible.

10. The method according to any one of the preceding claims, comprising the step of; computing the output of the auction such that the users learn, in addition, some statistic of the inputs, such as, the users can learn at least one of the average of the inputs, the variance of the inputs, or how many one inputs were in a certain range.

11. The method according to any one of the preceding claims, comprising the step of computing the output of the function such that only the center learns the output of the function. or several of the users learn the output of the function, or all the users learn the output of the function.

12. The method according to any one of the preceding claims, comprising the step of, computing the output of a mechanism, in particular, for one of Groves-Clark mechanisms, opinion polling and stable matching.

13. The method according to any one of the preceding claims, comprising the steps of each user committing to the values of his input in a manner that the user cannot change it afterwards, but hiding the input value from the center,.at a specific stage, the users opening their commitments to their inputs and revealing their values to the center, which then computes the value of F in a manner the each of the users can verify that the values that were used as inputs for computing F were the values that were committed to by the users.

14. The method according to any one of the preceding claims, comprising the step of implementing automated agents which participate in the auction which do not disclose to the auctioneer the limit price that they were given, until the end of the bidding period.

15. The method according to any one of the preceding claims, comprising the step of computing a function where the center can generate a proof that it computed the correct output of the function.

16. The method according to any one of the preceding claims, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties' inputs.

17. In a system that contains N parties, each having a private input, and a center adapted to compute a function F of said input; apparatus for computing said function F in said center, comprising:

a first program provided in the center that enables calculation of said function F;

circuitry for publishing said function F using the program while not revealing substantially any information about said input; and

a second program provided to the parties enabling each one of said parties to prove that said function F was calculated correctly.

18. In a system according to claim 17, wherein the second program precludes the learning of any information other than the function F was calculated correctly.

19. In a system according to claim 17, wherein the first program includes a construction of K garbled circuits for computing function F.

20. In a system according to claim 17, wherein said parties are bidders in an auction; said input are bids, said center is an auctioneer, said function F is the rule by which said auction is decided, whereby the auctioneer is capable of calculating the result of said auction without revealing any information about said bids, except for the identity of the winning party from among said parties, and the amount to pay.

21. In a system according to claim 20, wherein the function is determined utilizing a circuit of gates.

22. In a system according to claim 20, wherein the second program includes the capability of utilizing the circuit of gates to independently determine and verify that the computations of the center are correct.

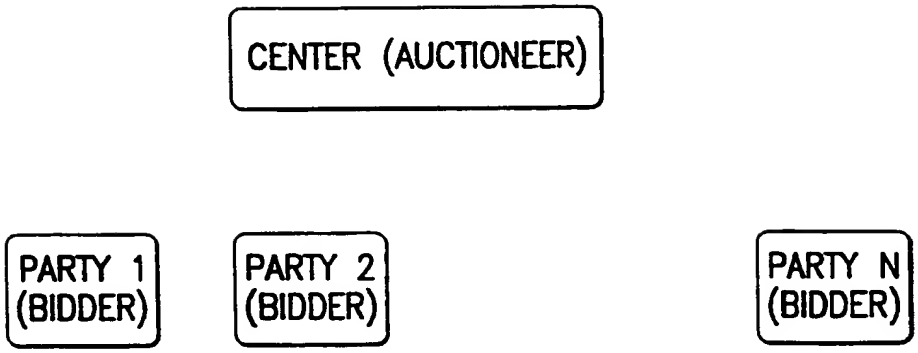

CENTER (AUCTIONEER)
PARTY 1 (BIDDER)
PARTY 2 (BIDDER)
PARTY N (BIDDER)

FIG.1

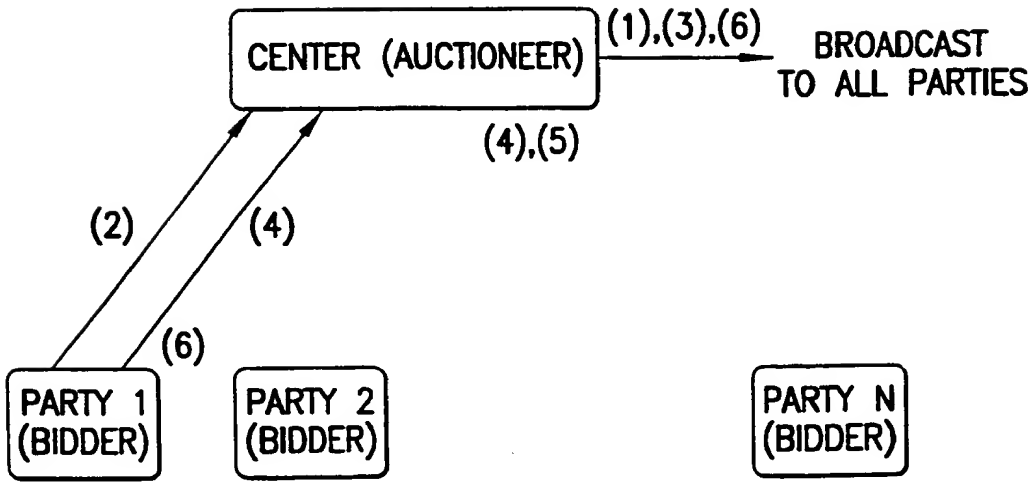

CENTER (AUCTIONEER)
(1),(3),(6)
BROADCAST TO ALL PARTIES
(4),(5)
(2)
(4)
(6)
PARTY 1 (BIDDER)
PARTY 2 (BIDDER)
PARTY N (BIDDER)

FIG.2

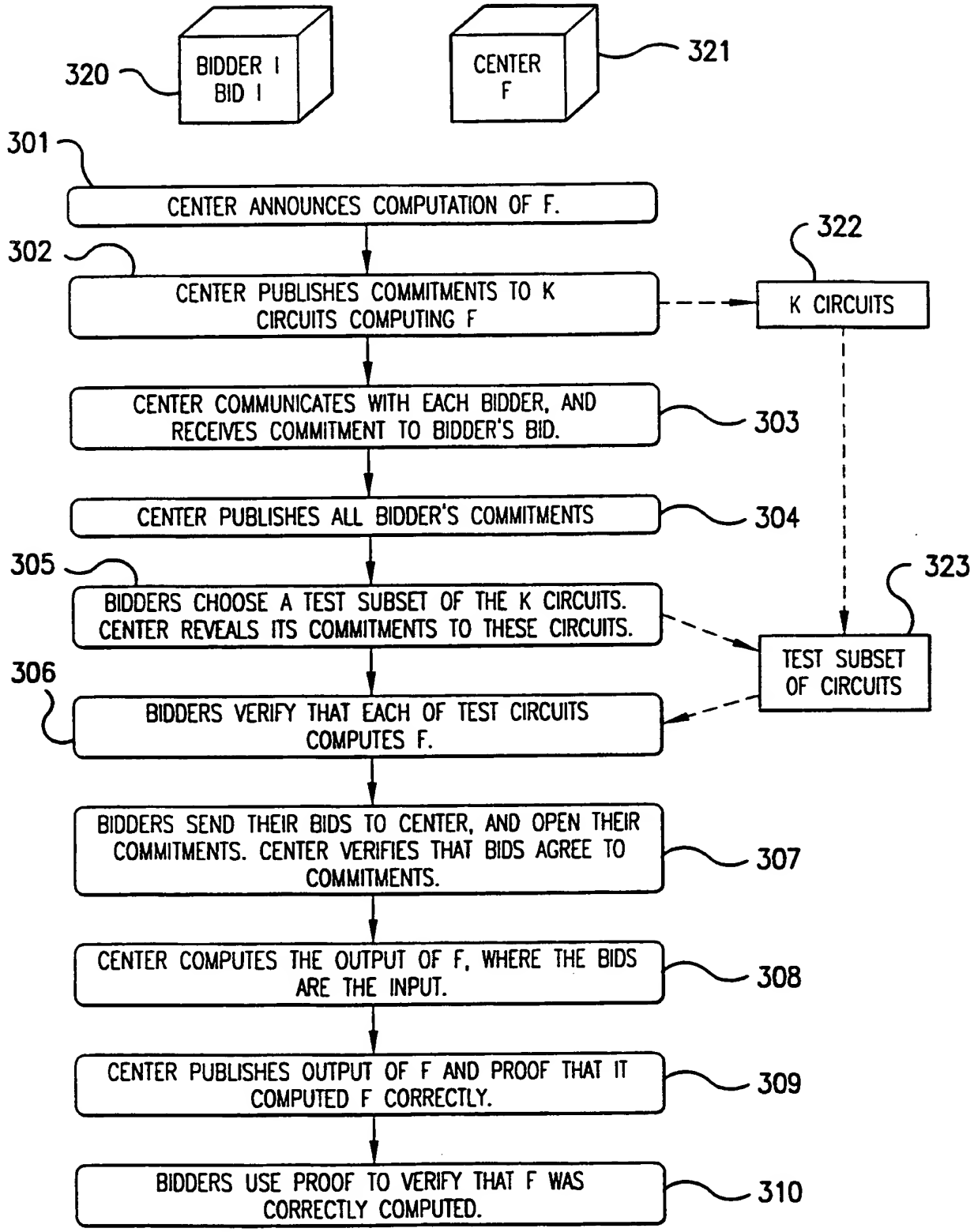

BIDDER I
BID I
320
CENTER
F
321
301
CENTER ANNOUNCES COMPUTATION OF F.
302
CENTER PUBLISHES COMMITMENTS TO K CIRCUITS COMPUTING F
322
K CIRCUITS
CENTER COMMUNICATES WITH EACH BIDDER, AND RECEIVES COMMITMENT TO BIDDER'S BID.
303
CENTER PUBLISHES ALL BIDDER'S COMMITMENTS
304
305
BIDDERS CHOOSE A TEST SUBSET OF THE K CIRCUITS. CENTER REVEALS ITS COMMITMENTS TO THESE CIRCUITS.
323
TEST SUBSET OF CIRCUITS
306
BIDDERS VERIFY THAT EACH OF TEST CIRCUITS COMPUTES F.
BIDDERS SEND THEIR BIDS TO CENTER, AND OPEN THEIR COMMITMENTS. CENTER VERIFIES THAT BIDS AGREE TO COMMITMENTS.
307
CENTER COMPUTES THE OUTPUT OF F, WHERE THE BIDS ARE THE INPUT.
308
CENTER PUBLISHES OUTPUT OF F AND PROOF THAT IT COMPUTED F CORRECTLY.
309
BIDDERS USE PROOF TO VERIFY THAT F WAS CORRECTLY COMPUTED.
310

FIG.3

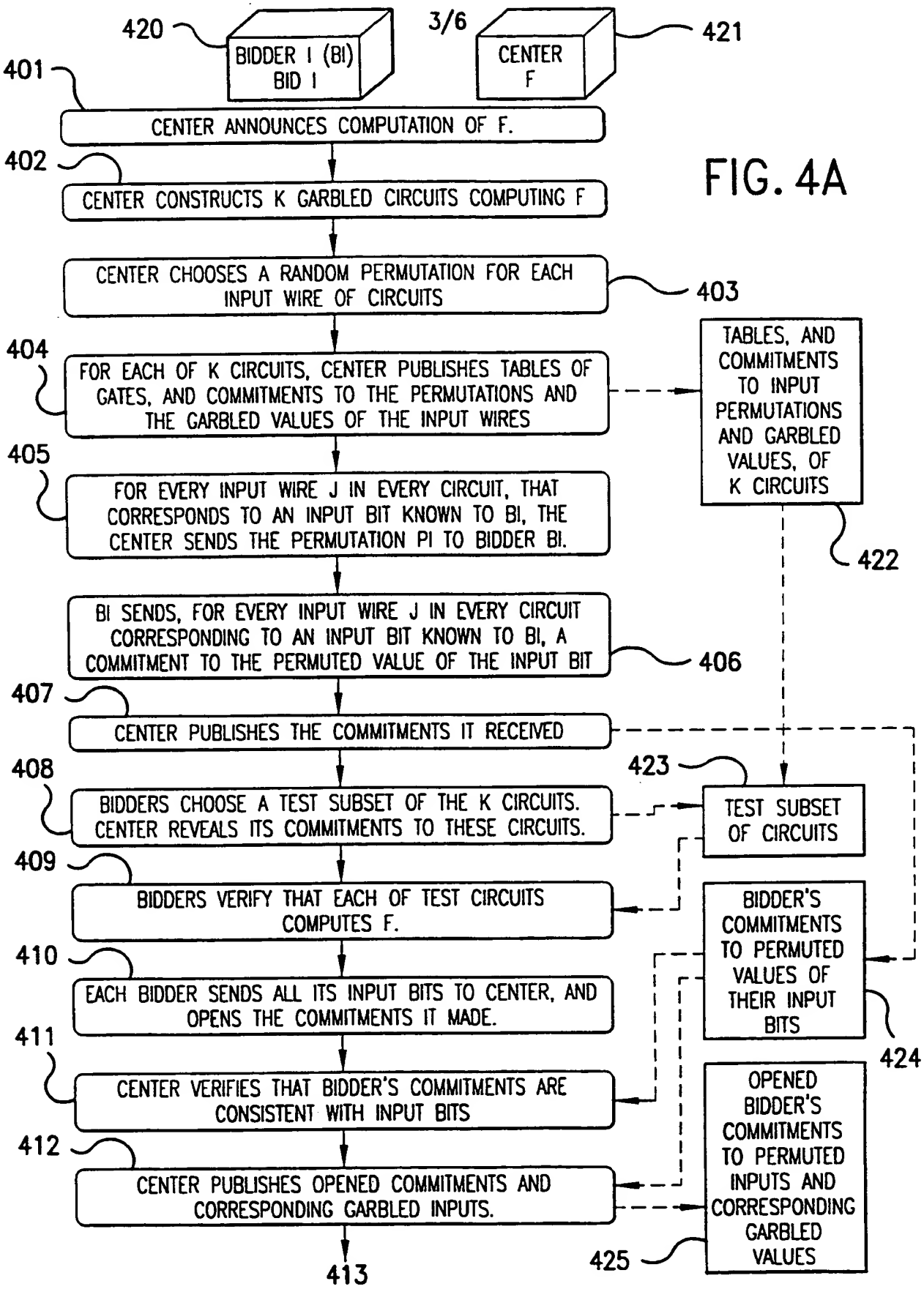

420
BIDDER I (BI)
BID I
CENTER
F
421
401
CENTER ANNOUNCES COMPUTATION OF F.
402
CENTER CONSTRUCTS K GARBLED CIRCUITS COMPUTING F
CENTER CHOOSES A RANDOM PERMUTATION FOR EACH INPUT WIRE OF CIRCUITS
403
404
FOR EACH OF K CIRCUITS, CENTER PUBLISHES TABLES OF GATES, AND COMMITMENTS TO THE PERMUTATIONS AND THE GARBLED VALUES OF THE INPUT WIRES
TABLES, AND COMMITMENTS TO INPUT PERMUTATIONS AND GARBLED VALUES, OF K CIRCUITS
422
405
FOR EVERY INPUT WIRE J IN EVERY CIRCUIT, THAT CORRESPONDS TO AN INPUT BIT KNOWN TO BI, THE CENTER SENDS THE PERMUTATION PI TO BIDDER BI.
BI SENDS, FOR EVERY INPUT WIRE J IN EVERY CIRCUIT CORRESPONDING TO AN INPUT BIT KNOWN TO BI, A COMMITMENT TO THE PERMUTED VALUE OF THE INPUT BIT
406
407
CENTER PUBLISHES THE COMMITMENTS IT RECEIVED
423
408
BIDDERS CHOOSE A TEST SUBSET OF THE K CIRCUITS. CENTER REVEALS ITS COMMITMENTS TO THESE CIRCUITS.
TEST SUBSET OF CIRCUITS
409
BIDDERS VERIFY THAT EACH OF TEST CIRCUITS COMPUTES F.
BIDDER'S COMMITMENTS TO PERMUTED VALUES OF THEIR INPUT BITS
424
410
EACH BIDDER SENDS ALL ITS INPUT BITS TO CENTER, AND OPENS THE COMMITMENTS IT MADE.
411
CENTER VERIFIES THAT BIDDER'S COMMITMENTS ARE CONSISTENT WITH INPUT BITS
412
CENTER PUBLISHES OPENED COMMITMENTS AND CORRESPONDING GARBLED INPUTS.
OPENED BIDDER'S COMMITMENTS TO PERMUTED INPUTS AND CORRESPONDING GARBLED VALUES
425
413

FIG. 4A

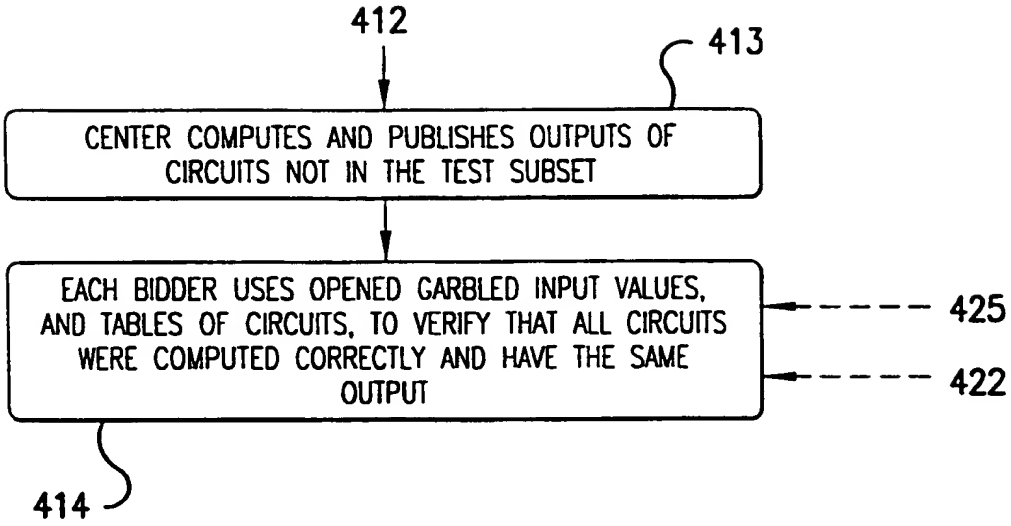

412
413
CENTER COMPUTES AND PUBLISHES OUTPUTS OF CIRCUITS NOT IN THE TEST SUBSET
EACH BIDDER USES OPENED GARBLED INPUT VALUES, AND TABLES OF CIRCUITS, TO VERIFY THAT ALL CIRCUITS WERE COMPUTED CORRECTLY AND HAVE THE SAME OUTPUT
425
422
414

FIG. 4B

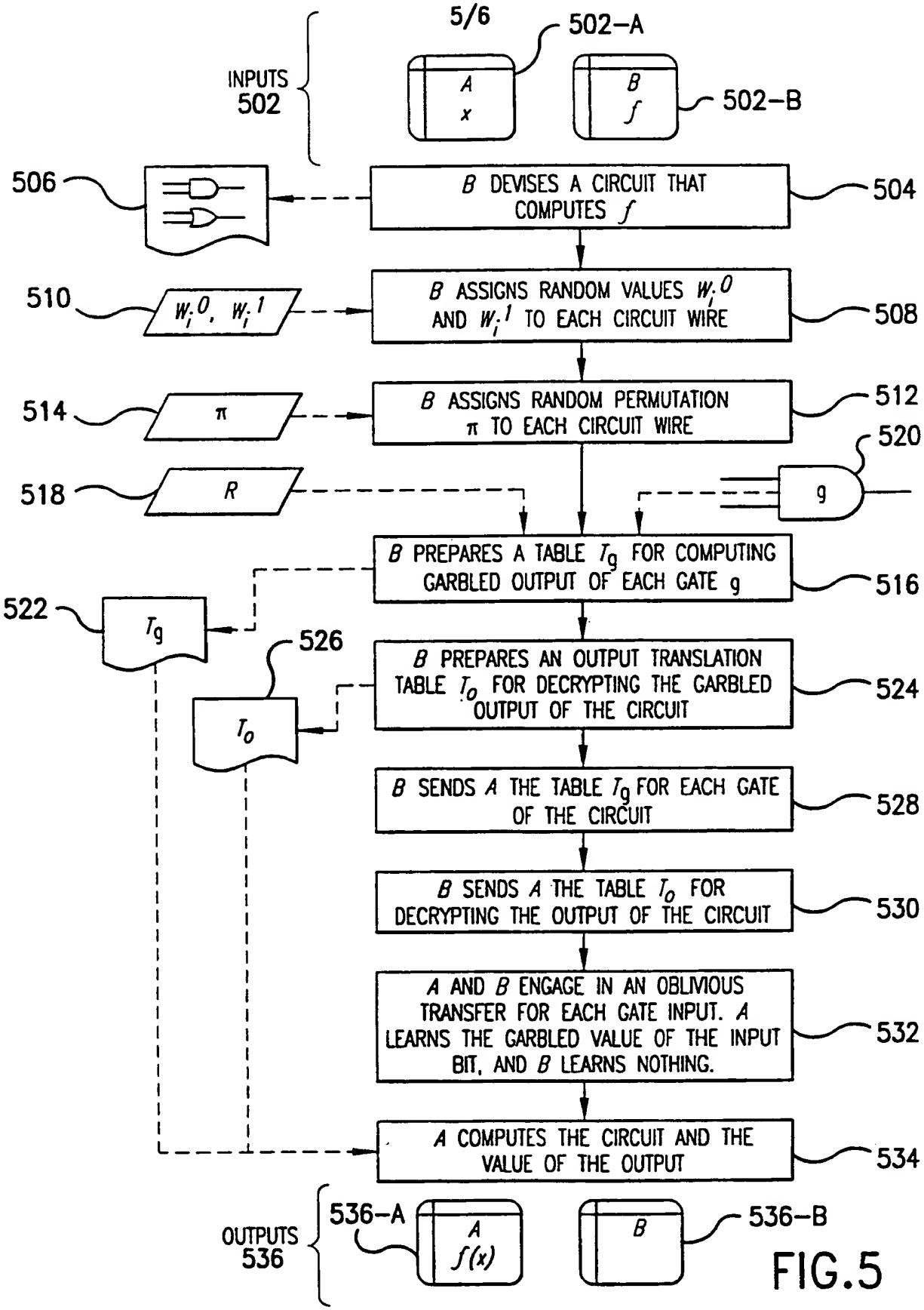

INPUTS 502
502-A
A x
B f
502-B
506
B DEVISES A CIRCUIT THAT COMPUTES f
504
510
W_i^0, W_i^1
B ASSIGNS RANDOM VALUES W_i^0 AND W_i^1 TO EACH CIRCUIT WIRE
508
514
π
B ASSIGNS RANDOM PERMUTATION π TO EACH CIRCUIT WIRE
512
518
R
520
g
B PREPARES A TABLE T_g FOR COMPUTING GARBLED OUTPUT OF EACH GATE g
516
522
T_g
526
T_o
B PREPARES AN OUTPUT TRANSLATION TABLE T_o FOR DECRYPTING THE GARBLED OUTPUT OF THE CIRCUIT
524
B SENDS A THE TABLE T_g FOR EACH GATE OF THE CIRCUIT
528
B SENDS A THE TABLE T_o FOR DECRYPTING THE OUTPUT OF THE CIRCUIT
530
A AND B ENGAGE IN AN OBLIVIOUS TRANSFER FOR EACH GATE INPUT. A LEARNS THE GARBLED VALUE OF THE INPUT BIT, AND B LEARNS NOTHING.
532
A COMPUTES THE CIRCUIT AND THE VALUE OF THE OUTPUT
534
OUTPUTS 536
536-A
A f(x)
B
536-B

FIG.5

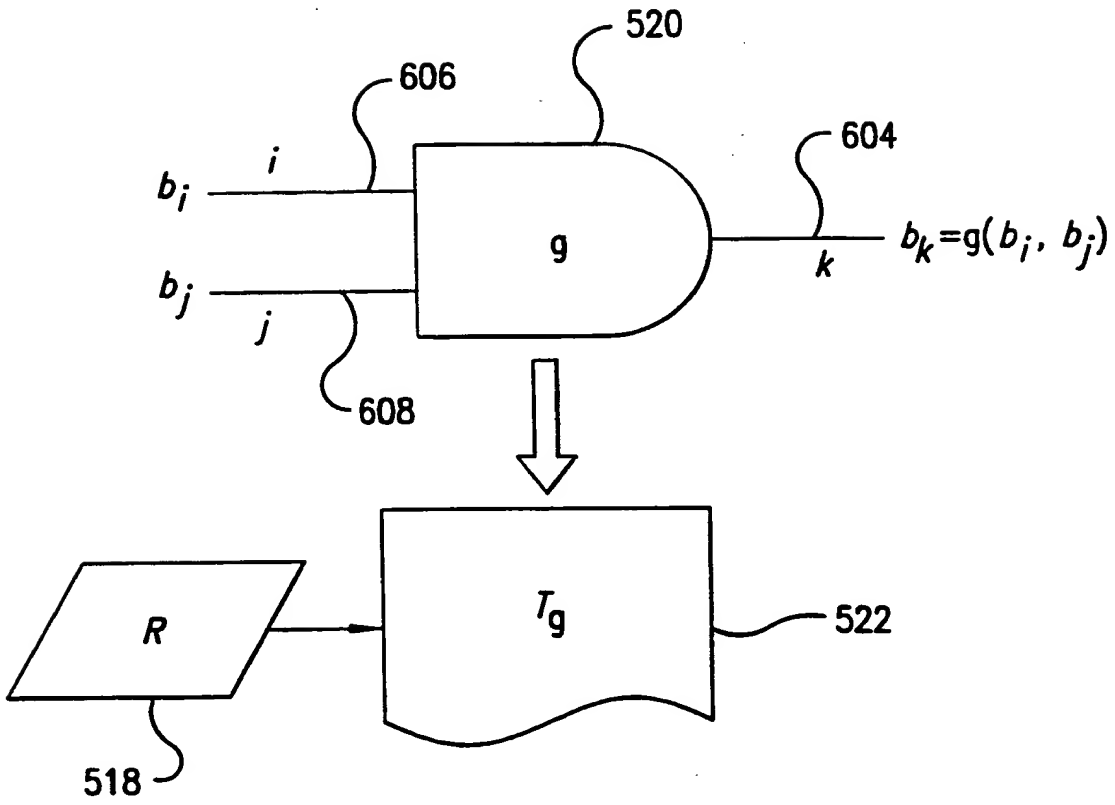


FIG.6

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference	IMPORTANT DECLARATION	Date of mailing *(day/month/year)*
704-X00-047		01/10/2001
International application No.	International filing date *(day/month/year)*	(Earliest) Priority date *(day/month/year)*
PCT/US 00/ 21615	08/08/2000	10/08/1999
International Patent Classification (IPC) or both national classification and IPC	G06F17/60	
Applicant		
YEDA RESEARCH AND DEVELOPMENT CO. LTD.		

This International Searching Authority hereby declares, according to Article 17(2)(a), that **no international search report will be established** on the international application for the reasons indicated below

1. [X] The subject matter of the international application relates to:
   - a. [ ] scientific theories.
   - b. [ ] mathematical theories
   - c. [ ] plant varieties.
   - d. [ ] animal varieties.
   - e. [ ] essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
   - f. [X] schemes, rules or methods of doing business.
   - g. [ ] schemes, rules or methods of performing purely mental acts.
   - h. [ ] schemes, rules or methods of playing games.
   - i. [ ] methods for treatment of the human body by surgery or therapy.
   - j. [ ] methods for treatment of the animal body by surgery or therapy.
   - k. [ ] diagnostic methods practised on the human or animal body.
   - l. [ ] mere presentations of information.
   - m. [ ] computer programs for which this International Searching Authority is not equipped to search prior art.

2. [ ] The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
   [ ] the description [ ] the claims [ ] the drawings

3. [ ] The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
   [ ] the written form has not been furnished or does not comply with the standard.
   [ ] the computer readable form has not been furnished or does not comply with the standard.

4. Further comments:

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lucia Van Pinxteren

Form PCT/ISA/203 (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 203

The subject-matter claimed in claims 1-16 falls under the provisions of Article 17(2)(a)(i) and Rule 39.1 (i),(iii) PCT, such subject-matter relating to scientific and mathematical theories and to a method of doing business.

Claims 17-22 relate to commonplace technological features for implementing the scientific theories and performing the business method of the method claims. Although these claims do not literally belong to the method category, they essentially claim protection for the same commercial effect as the method claims. With reference to the Guidelines, B-VIII, points 1-6, the International Searching Authority considers that searching such commercial features would serve no useful purpose. This applies to the remaining commonplace technological features of these claims as well.

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

PCT

REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

International Application No.

International Filing Date

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)* 704-X00-047

Box No. I TITLE OF INVENTION

HONESTY PRESERVING NEGOTIATION AND COMPUTATION

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

YEDA RESEARCH AND DEVELOPMENT CO. LTD.
P.O. BOX 95
REHOVOT 76100
ISRAEL

☐ This person is also inventor.

Telephone No. 972-8-947-0617

Facsimile No. 972-9-947-0739

Teleprinter No.

State *(that is, country)* of nationality: ISRAEL

State *(that is, country)* of residence: ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☒ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

FLEIT, LOIS
520 BRICKELL KEY DRIVE #A201
MIAMI, FLORIDA 33131
USA

This person is:

☒ applicant only

☐ applicant and inventor

☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: USA

State *(that is, country)* of residence: USA

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☒ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet.

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

FLEIT, MARTIN REG. NO. 16,900
FLEIT KAIN GIBBONS GUTMAN & BONGINI
520 BRICKELL KEY DRIVE #A201
MIAMI, FLORIDA 33131 USA

Telephone No. 305-536-9020

Facsimile No. 305-536-9022

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

Continuation of Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)

If none of the following sub-boxes is used, this sheet should not be included in the request.

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

PINKAS, BINYAMIN
6 EIBESHITZ STREET
TEL-AVIV 62741

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: ISRAEL

State *(that is, country)* of residence: ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

NAOR, SIMEON
5 BEIT STREET
TEL-AVIV 69122
ISRAEL

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: ISRAEL

State *(that is, country)* of residence: ISRAEL

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

Box No. V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

- ☐ AP ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☐ EA Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ EP European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☐ OA OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☐ AE	United Arab Emirates	☐ LC	Saint Lucia
☐ AG	Antigua and Barbuda	☐ LK	Sri Lanka
☐ AL	Albania	☐ LR	Liberia
☐ AM	Armenia	☐ LS	Lesotho
☐ AT	Austria	☐ LT	Lithuania
☐ AU	Australia	☐ LU	Luxembourg
☐ AZ	Azerbaijan	☐ LV	Latvia
☐ BA	Bosnia and Herzegovina	☐ MA	Morocco
☐ BB	Barbados	☐ MD	Republic of Moldova
☐ BG	Bulgaria	☐ MG	Madagascar
☐ BR	Brazil	☐ MK	The former Yugoslav Republic of Macedonia
☐ BY	Belarus	☐ MN	Mongolia
☐ BZ	Belize	☐ MW	Malawi
☒ CA	Canada	☐ MX	Mexico
☐ CH and LI	Switzerland and Liechtenstein	☐ MZ	Mozambique
☐ CN	China	☐ NO	Norway
☐ CR	Costa Rica	☐ NZ	New Zealand
☐ CU	Cuba	☐ PL	Poland
☐ CZ	Czech Republic	☐ PT	Portugal
☐ DE	Germany	☐ RO	Romania
☐ DK	Denmark	☐ RU	Russian Federation
☐ DM	Dominica	☐ SD	Sudan
☐ DZ	Algeria	☐ SE	Sweden
☐ EE	Estonia	☐ SG	Singapore
☐ ES	Spain	☐ SI	Slovenia
☐ FI	Finland	☐ SK	Slovakia
☐ GB	United Kingdom	☐ SL	Sierra Leone
☐ GD	Grenada	☐ TJ	Tajikistan
☐ GE	Georgia	☐ TM	Turkmenistan
☐ GH	Ghana	☐ TR	Turkey
☐ GM	Gambia	☐ TT	Trinidad and Tobago
☐ HR	Croatia	☐ TZ	United Republic of Tanzania
☐ HU	Hungary	☐ UA	Ukraine
☐ ID	Indonesia	☐ UG	Uganda
☒ IL	Israel	☒ US	United States of America
☐ IN	India	☐ UZ	Uzbekistan
☐ IS	Iceland	☐ VN	Viet Nam
☒ JP	Japan	☐ YU	Yugoslavia
☐ KE	Kenya	☐ ZA	South Africa
☐ KG	Kyrgyzstan	☐ ZW	Zimbabwe
☐ KP	Democratic People's Republic of Korea	Check-box reserved for designating States which have become party to the PCT after issuance of this sheet:	
☐ KR	Republic of Korea	☐	
☐ KZ	Kazakhstan		

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Supplemental Box *If the Supplemental Box is not used, this sheet should not be included in the request.*

1. If, in any of the Boxes, the space is insufficient to furnish all the information: in such case, write "Continuation of Box No. ..." [indicate the number of the Box] and furnish the information in the same manner as required according to the captions of the Box in which the space was insufficient, in particular:

(i) if more than two persons are involved as applicants and/or inventors and no "continuation sheet" is available: in such case, write "Continuation of Box No. III" and indicate for each additional person the same type of information as required in Box No. III. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below;

(ii) if, in Box No. II or in any of the sub-boxes of Box No. III, the indication "the States indicated in the Supplemental Box" is checked: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the applicant(s) involved and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is applicant;

(iii) if, in Box No. II or in any of the sub-boxes of Box No. III, the inventor or the inventor/applicant is not inventor for the purposes of all designated States or for the purposes of the United States of America: in such case, write "Continuation of Box No. II" or "Continuation of Box No. III" or "Continuation of Boxes No. II and No. III" (as the case may be), indicate the name of the inventor(s) and, next to (each) such name, the State(s) (and/or, where applicable, ARIPO, Eurasian, European or OAPI patent) for the purposes of which the named person is inventor;

(iv) if, in addition to the agent(s) indicated in Box No. IV, there are further agents: in such case, write "Continuation of Box No. IV" and indicate for each further agent the same type of information as required in Box No. IV;

(v) if, in Box No. V, the name of any State (or OAPI) is accompanied by the indication "patent of addition," or "certificate of addition," or if, in Box No. V, the name of the United States of America is accompanied by an indication "continuation" or "continuation-in-part": in such case, write "Continuation of Box No. V" and the name of each State involved (or OAPI), and after the name of each such State (or OAPI), the number of the parent title or parent application and the date of grant of the parent title or filing of the parent application;

(vi) if, in Box No. VI, there are more than three earlier applications whose priority is claimed: in such case, write "Continuation of Box No. VI" and indicate for each additional earlier application the same type of information as required in Box No. VI;

(vii) if, in Box No. VI, the earlier application is an ARIPO application: in such case, write "Continuation of Box No. VI", specify the number of the item corresponding to that earlier application and indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed.

2. If, with regard to the precautionary designation statement contained in Box No. V, the applicant wishes to exclude any State(s) from the scope of that statement: in such case, write "Designation(s) excluded from precautionary designation statement" and indicate the name or two-letter code of each State so excluded.

3. If the applicant claims, in respect of any designated Office, the benefits of provisions of the national law concerning non-prejudicial disclosures or exceptions to lack of novelty: in such case, write "Statement concerning non-prejudicial disclosures or exceptions to lack of novelty" and furnish that statement below.

CONTINUATION OF BOXES NO. II AND NO. III

FLEIT, LOIS : CA

YEDA RESEARCH AND DEVELOPMENT CO. LTD. : EP, IL, JP AND US

CONTINUATION OF BOX IV

KAIN, ROBERT C.; GIBBONS, JON A.; GUTMAN, JOSE; BONGINI, STEPHEN C.. THE ADDRESS OF THE MENTIONED AGENTS IS THE SAME AS THAT LISTED IN BOX IV.

Sheet No. .....

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplemental Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) 10/08/99	60/148,183	US		
item (2)				
item (3)				

☒ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): _____

** Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)* :

ISA / EP

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date *(day/month/year)* Number Country *(or regional Office)*

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets**:

request	: 5
description (excluding sequence listing part)	: 16
claims	: 4
abstract	: 1
drawings	: 6
sequence listing part of description	:
Total number of sheets	: 32

This international application is **accompanied** by the item(s) marked below:

1. ☒ fee calculation sheet
2. ☐ separate signed power of attorney
3. ☐ copy of general power of attorney; reference number, if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international application into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listing in computer readable form
9. ☒ other *(specify)*: TRANSMITTAL

Figure of the drawings which should accompany the abstract: FIG. 2

Language of filing of the international application: ENGLISH

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

MARTIN FLEIT, REG. NO. 16,900

For receiving Office use only

1. Date of actual receipt of the purported international application:
2. Drawings: ☐ received: ☐ not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:
4. Date of timely receipt of the required corrections under PCT Article 11(2):
5. International Searching Authority (if two or more are competent): ISA /
6. ☐ Transmittal of search copy delayed until search fee is paid.

For International Bureau use only

Date of receipt of the record copy by the International Bureau: